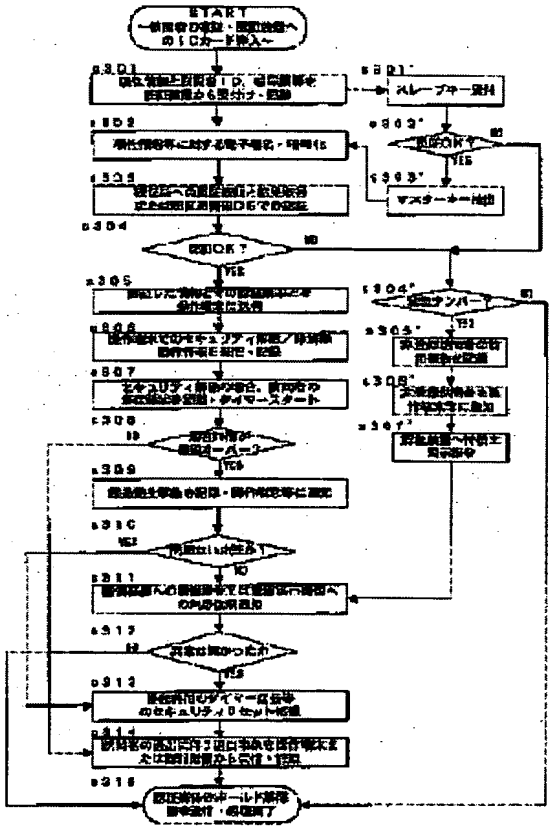
METHOD AND SYSTEM OR CONTROLLING SECURITY VIA NETWORK

Patent number: JP2003141664
Publication date: 2003-05-16
Inventor: YAMADA DAIJI; TAKAHASHI NAOKI
Applicant: HITACHI LTD
Classification:
- international: ***G06F15/00; G08B25/04; H04L9/32;*** **G06F15/00; G08B25/01; H04L9/32;** (IPC1-7): G08B25/04; G06F15/00; H04L9/32
- european:
Application number: JP20010342469 20011107
Priority number(s): JP20010342469 20011107

Abstract of **JP2003141664**

PROBLEM TO BE SOLVED: To provide a method and a system for controlling security capable of restraining easily and surely the generation of an intrusion matter and the like at a low cost, and rich in flexibility for function expansion. SOLUTION: This method (system) executes an ID-and-the-like receiving procedure s301 for receiving attribute information, from an identifier, provided by an reading operation to an identification medium and a visitor ID provided by receiving an input in the identifier, an identification procedure s303 for recording the visitor ID and the attribute information in a database, and for identifying the rightness of a corresponding visitor by executing the identification in the database recorded with the visitor ID while corresponding to the visitor or the recording medium individually, or by making a request an identification station that is an origin of the visitor ID for identification, and a result thereof, a security-release-and-the- like recording procedure s306 for transmitting the result of identification processing to an operation terminal, and for receiving, from the operation terminal, release/non-release operation information for the security in the operation terminal in response to the propriety of acceptance of the visitor within a control boundary, to be recorded in the database, and a leaving recording procedure s315 for receiving a leaving event of the visitor from the identifier or the like to be recorded in the database, and for transmitting a holding release command to the identification medium to the identifier or the like.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－141664
（P2003－141664A）
(43)公開日　平成15年５月16日(2003.5.16)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０８Ｂ　25/04		Ｇ０８Ｂ　25/04	Ｆ　５Ｂ０８５
			Ｇ　５Ｃ０８７
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ　５Ｊ１０４
			３３０Ｇ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ

審査請求　未請求　請求項の数９　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願2001－342469(P2001－342469)

(22)出願日　平成13年11月７日(2001.11.7)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

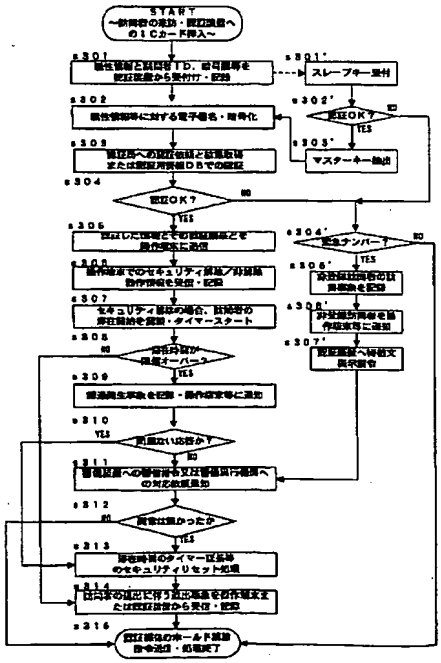
(72)発明者　山田　大二
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション事業部内

(74)代理人　100071283
弁理士　一色　健輔　（外５名）

最終頁に続く

(54)【発明の名称】　ネットワークを介したセキュリティ管理方法およびシステム

(57)【要約】
【課題】　侵入事件等の発生を簡便確実かつ低コストのもとで抑制し、機能拡張等の柔軟性に富んだセキュリティ管理方法およびシステムを提供する。
【解決手段】　認証媒体に対する読込み動作により得られた属性情報と認証装置における入力を受け付けて得た訪問者ＩＤとを認証装置から受付けるＩＤ等受付手順ｓ３０１と、訪問者ＩＤと属性情報とをデータベースに記録すると共に訪問者又は認証媒体各個に対応付けて訪問者ＩＤを記録したデータベースにおける認証又は訪問者ＩＤの起源となっている認証局への認証依頼とその結果の取得を実行することで該当訪問者の正当性を認証する認証手順ｓ３０３と、認証処理の結果を操作端末に送信すると共に管理境界内への訪問者の受け入れ可否に応じて当該操作端末でのセキュリティの解除／非解除動作情報を操作端末から受信してデータベースに記録するセキュリティ解除等記録手順ｓ３０６と、訪問者の退出事象を認証装置等から受信してデータベースに記録すると共に認証媒体に対するホールド解除指令を認証装置等に送信する退出記録手順ｓ３１５とを実行する。



1

【特許請求の範囲】

【請求項１】　建造物或いは建造物内外の特定エリアの管理境界における訪問者の出入管理を、ネットワークを介してサーバーが行うセキュリティ管理の方法であって、

訪問者個々に割り当てられたＩＤと当該訪問者の属性情報とを少なくとも記録している認証媒体に対する、前記管理境界に設置された認証装置による読み込み動作によって得られた属性情報と、当該訪問者による認証装置における入力を受け付けて得た訪問者ＩＤとを、この認証装置から受付けるＩＤ等受付手順と、

前記認証装置から受け付けた訪問者ＩＤと属性情報とをデータベースに記録するとともに、訪問者あるいは認証媒体各個に対応付けて訪問者ＩＤを記録したデータベースにおける認証、または前記訪問者ＩＤの起源となっている認証局への認証依頼とその結果の取得を実行することで該当訪問者の正当性を認証する認証手順と、

前記認証処理の結果を、該当管理境界内に設置されている操作端末に送信すると共に、管理境界内への訪問者の受け入れ可否に応じて当該操作端末で行われたセキュリティの解除／非解除動作情報を操作端末から受信してデータベースに記録するセキュリティ解除等記録手順と、

受け入れられた訪問者が管理境界から退出する旨を示す退出事象を前記操作端末または認証装置から受信してこれをデータベースに記録すると共に、この訪問者の認証媒体に対するホールド解除指令を操作端末または認証装置に送信する退出記録手順とを備えることを特徴とするセキュリティ管理方法。

【請求項２】　前記ＩＤ等受付手順において、訪問者個々に割り当てられた暗号鍵と当該訪問者の属性情報とを記録している認証媒体に対する、前記認証装置による読み込み動作によって得られた属性情報と、当該訪問者による認証装置における入力を受け付けて得た暗号鍵と、この暗号鍵で電子署名を施した署名付き属性情報とを、この認証装置から受付け、

前記認証手順において、前記暗号鍵および署名付き属性情報をデータベースに記録すると共に、当該暗号鍵と署名付き属性情報とを認証局に送信してその認証結果を入手することで該当訪問者の正当性を認証することを特徴とする請求項１に記載のセキュリティ管理方法。

【請求項３】　サーバーが、訪問者になるであろう登録者に所定間隔でスレーブキーを更新発行し、このスレーブキーに関する認証装置における訪問者の入力を受付けて一次認証を行うと共に、このスレーブキーに対応する登録者に対して認証局から発行されたマスターキーをデータベースから抽出して認証局に送信し、その認証結果を取得する二次認証を実行することを特徴とする請求項１または２に記載のセキュリティ管理方法。

【請求項４】　セキュリティ解除情報を記録した時点から、管理境界内における該当訪問者の滞在時間が開始し

2

たと認識し、この滞在時間が予め定めた閾値を越えた場合、その閾値超過発生事象を、該当する操作端末または認証装置に通知する超過発生事象通知手順と、

通知した超過発生事象に対する、操作端末または認証装置からの応答情報を受信して或いは応答情報の有無でもって、管理境界内での異常発生の有無を判断する異常発生判断手順と、

異常が発生していると判断したならば、管理境界に設置された所定の警備装置に適宜な警備動作を行うべく警備指令を通知するか、或いは、警察や予め契約してある警備会社等の警備実行機関に対処依頼通知を行う対応通知手順とを含むことを特徴とする請求項１～３のいずれかに記載のセキュリティ管理方法。

【請求項５】　前記ＩＤ等受付手順において受け付けた、訪問者ＩＤ、暗号鍵、またはスレーブキーのいずれかが、登録済みの正当な訪問者が緊急時に入力すべき緊急コードである場合、これを認証装置または操作端末から受け付けたサーバーは、非登録の訪問者である旨を前記操作端末に通知すると共に、前記対応通知手順を実行することを特徴とする請求項１～４のいずれかに記載のセキュリティ管理方法。

【請求項６】　建造物或いは建造物内外の特定エリアといったセキュリティ管理の対象が存在するエリア毎に担当警備会社や警察等の警備実行機関を関連づけするとし、当該警備実行機関の備える警備機関端末に対し、担当エリアに存在する操作端末または認証装置に対しなされる各種情報や指令の通知や記録手順を同様に実行することを特徴とする請求項１～５のいずれかに記載のセキュリティ管理方法。

【請求項７】　請求項１～６のいずれかのセキュリティ管理方法を実現するシステムであって、

訪問者個々に割り当てられたＩＤと当該訪問者の属性情報とを少なくとも記録している認証媒体に対する、前記管理境界に設置された認証装置による読み込み動作によって得られた属性情報と、当該訪問者による認証装置における入力を受け付けて得た訪問者ＩＤとを、この認証装置から受付けるＩＤ等受付装置と、

前記認証装置から受け付けた訪問者ＩＤと属性情報とをデータベースに記録するとともに、訪問者あるいは認証媒体各個に対応付けて訪問者ＩＤを記録したデータベースにおける認証、または前記訪問者ＩＤの起源となっている認証局への認証依頼とその結果の取得を実行することで該当訪問者の正当性を認証する認証装置と、

前記認証処理の結果を、該当管理境界内に設置されている操作端末に送信すると共に、管理境界内への訪問者の受け入れ可否に応じて当該操作端末で行われたセキュリティの解除／非解除動作情報を操作端末から受信してデータベースに記録するセキュリティ解除等記録装置と、

受け入れられた訪問者が管理境界から退出する旨の事象を前記操作端末または認証装置から受信してこれをデー

タベースに記録すると共に、この訪問者の認証媒体に対するホールド解除指令を操作端末または認証装置に送信する退出記録装置とを備えることを特徴とするセキュリティ管理システム。

【請求項８】　建造物或いは建造物内外の特定エリアの管理境界における訪問者の出入管理を、ネットワークを介したサーバー上で実現するプログラムであって、

訪問者個々に割り当てられたＩＤと当該訪問者の属性情報とを少なくとも記録している認証媒体に対する、前記管理境界に設置された認証装置による読み込み動作によって得られた属性情報と、当該訪問者による認証装置における入力を受け付けて得た訪問者ＩＤとを、この認証装置から受付けるＩＤ等受付手順と、

前記認証装置から受け付けた訪問者ＩＤと属性情報とをデータベースに記録するとともに、訪問者あるいは認証媒体各個に対応付けて訪問者ＩＤを記録したデータベースにおける認証、または前記訪問者ＩＤの起源となっている認証局への認証依頼とその結果の取得を実行することで該当訪問者の正当性を認証する認証手順と、

前記認証処理の結果を、該当管理境界内に設置されている操作端末に送信すると共に、管理境界内への訪問者の受け入れ可否に応じて当該操作端末で行われたセキュリティの解除／非解除動作情報を操作端末から受信してデータベースに記録するセキュリティ解除等記録手順と、

受け入れられた訪問者が管理境界から退出する旨の事象を前記操作端末または認証装置から受信してこれをデータベースに記録すると共に、この訪問者の認証媒体に対するホールド解除指令を操作端末または認証装置に送信する退出記録手順とを備えることを特徴とするセキュリティ管理プログラム。

【請求項９】　請求項８に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、建造物或いは建造物内外の特定エリアの管理境界における訪問者の出入管理を、ネットワークを介してサーバーが行うセキュリティ管理の方法に関する。

【０００２】

【発明の背景】宅配等を装って住宅内に押し入るといった事件が発生しており、個々の防犯意識が充分とは言えない我が国では社会問題化しつつある。そこで玄関錠を高性能なものと取り替えてそれにテレビ監視システムを連動させる、或いは窓や特定のエリアにモーションセンサーや人感ライトを設置するといった対策を講じる動きが注目されている。また、そのような監視装置を警備会社等と結んでリアルタイムにモニターし、何かしらの異常が発生したならば警備員を急行させるといったサービスも提供されている。

【０００３】

【発明が解決しようとする課題】しかしながら、従来のセキュリティシステムには、解決すべき余地が残されていた。まず言えるのがシステム導入にかかるコストである。大企業や多くのテナントを擁する大型ビルなどであれば、優れた防犯実績を誇る高機能のセキュリティシステムを全館的に導入することも容易であろうが、一般の個人住宅や中小企業など資力が十分とは言いにくい者にとっては、セキュリティシステムに多額の資金投入を行う訳にもいかない。

【０００４】翻って考えれば、例えば宅配等を装った侵入事件の多くが発生し、今後のセキュリティシステム導入が大きく見込まれるのが個人住宅等であるのに、当該個人住宅や中小企業等にとって導入コストという大きなハードルが存在していたのである。また、着目すべき課題として、従来のセキュリティシステムが対応しているのは、不審者がドア等から侵入し居室に入られたといった様な“発生後”の異常がほとんであり、それを未然に防止する策が低コストで提供されることは少なかった。

【０００５】またせっかくセキュリティシステムを導入しても状況の変化に応じて機能を拡張したり改変する柔軟性に優れず、システムに求める機能が変化したならばシステム全体の刷新を行うほかなかった。

【０００６】そこで本発明はこのような従来の課題に着目してなされたもので、侵入事件等の発生を簡便確実かつ低コストのもとで抑制し、機能拡張等の柔軟性に富んだセキュリティ管理方法およびシステムを提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成する本発明のセキュリティ管理方法は、建造物或いは建造物内外の特定エリアの管理境界における訪問者の出入管理を、ネットワークを介してサーバーが行うセキュリティ管理の方法であって、訪問者個々に割り当てられたＩＤと当該訪問者の属性情報とを少なくとも記録している認証媒体に対する、前記管理境界に設置された認証装置による読み込み動作によって得られた属性情報と、当該訪問者による認証装置における入力を受け付けて得た訪問者ＩＤとを、この認証装置から受付けるＩＤ等受付手順と、前記認証装置から受け付けた訪問者ＩＤと属性情報とをデータベースに記録するとともに、訪問者あるいは認証媒体各個に対応付けて訪問者ＩＤを記録したデータベースにおける認証、または前記訪問者ＩＤの起源となっている認証局への認証依頼とその結果の取得を実行することで該当訪問者の正当性を認証する認証手順と、認証処理の結果を、該当管理境界内に設置されている操作端末に送信すると共に、管理境界内への訪問者の受け入れ可否に応じて当該操作端末で行われたセキュリティの解除／非解除動作情報を操作端末から受信してデータベースに記録するセキュリティ解除等記録手順と、受け入れられた訪問者が管理境界から退出する旨を示す退出事象を

前記操作端末または認証装置から受信してこれをデータベースに記録すると共に、この訪問者の認証媒体に対するホールド解除指令を認証装置に送信する退出記録手順とを備えることを特徴とする。

【０００８】

【発明の実施の形態】以下に本発明の実施形態について図面を用いて詳細に説明する。図１は本実施形態におけるセキュリティ管理システムとしてのＡＳＰサーバー１０を含むネットワーク概要図であり、図２は本実施形態におけるセキュリティ管理方法を適用したビジネスモデルを示す説明図である。この実施例の背景として、本発明のセキュリティ管理方法を適用したセキュリティサービスを提供する管理会社が、サービス契約を結んだ契約住宅における出入管理を、予め登録された訪問業者の構成員に関する認証作業をベースに行うと共に、地域ごとに散在するローカル警備会社や警察機構を介して実際の警備活動のサービス提供をも実現する状況を想定する。勿論、本実施例だけに本発明の適用範囲が限定されるものではなく、ネットワークを通じて出入管理を行ういずれの状況にも本発明を適用することが可能であるのは言うまでもない。

【０００９】本発明を実現するＡＳＰサーバー１０は、前記管理会社が運営・管理しているサーバーであって、例えばセキュリティサービスを提供する管轄エリア毎に運営される。そして、イントラネットやインターネット、或いは公衆回線網など各種の通信回線網と接続してそのプロトコルに則ったデータ通信を実行する通信装置を付帯させている。当該ＡＳＰサーバー１０はこの通信装置を介し、契約住宅における操作端末２０や認証装置２５、或いは契約者が所持する携帯端末２７、並びに登録された前記訪問会社の登録会社端末６０等と訪問者ＩＤや属性情報等の各種データや認証結果等の送受信を処理する一方で、認証局サーバー３０から認証結果を受信し、警察端末４０や（ローカル警備会社の）警備会社端末５０への対処依頼通知などを行う。勿論ＡＳＰサーバー１０は、ファイヤウォールサーバとして外部からの不正進入を抑止したり、WWWサーバとして機能するものでもあるし、データ通信相手とのコミュニケーションを図るメールサーバーとしても機能可能なものである。

【００１０】このようなＡＳＰサーバー１０は、データベースとして例えば認証用情報データベース１１や動作記録データベース１２を備えている。認証用情報データベース１１は、前記管理会社が予め契約を結んでいる（宅配業等を生業とする）訪問会社についてその各構成員（以下、単に訪問者）毎に割り当てた訪問者ＩＤに、属性情報を絡めて管理している。この属性情報とは、例えば所属訪問会社名、所在地、連絡先、所属部署、担当管理者、社員ナンバー、生年月日など当該訪問者の所属する訪問会社に由来する情報や個人情報が含まれている。またこの認証用情報データベース１１では、例えば、契約住宅毎に、または訪問会社毎に或いは訪問会社の業種毎に、１回の訪問者の契約住宅内での適度な滞在時間を設定したタイムテーブルも管理している。

【００１１】他に訪問者ＩＤに関係付けして登録管理する情報として、訪問者個々に割り当てられた暗号鍵情報がある。この暗号鍵情報は、例えば公開鍵インフラ（いわゆるＰＫＩ）をベースに訪問者の出入管理を行うとすれば、認証装置２５や操作端末２０とＡＳＰサーバー１０との間、或いはＡＳＰサーバー１０と認証局サーバー３０との間など種々のデータ通信を行う際に、やり取りするデータに電子署名を施すことでデータ改竄の有無を検証可能とし、更に認証局による確実な訪問者認証を実現する。もちろん、通信の暗号化を図ってデータ漏洩を抑止することにもつながる。また、本発明では、この暗号鍵を、例えば毎日といった所定間隔で訪問者に発行するスレーブキーと、このスレーブキーが関係付けられた認証局発行のマスターキーとの２種に分けて考えることも出来る。

【００１２】他方、動作記録データベース１２は、訪問者或いは非登録の訪問者が契約住宅を訪れたことに起因する、操作端末２０、認証装置２５、携帯端末２７、ＡＳＰサーバー１０、認証局サーバー３０、警察端末４０、警備会社端末５０、または登録会社端末６０の少なくともいずれかでの処理事象や動作状況を記録するものである。この動作記録データベース１２は、例えば契約住宅毎にデータ構成することとし、当該契約住宅に対応した契約者が操作する操作端末２０や携帯端末２７からの情報閲覧を受け付けて、留守宅で生じた様々な事象をリアルタイムに或いは後に提供することが可能である。なお、この動作記録データベース１２は、契約住宅毎に個別設置せれるとし、操作端末２０と一体になっているとしても問題ない。

【００１３】一方、契約住宅に設置されているのが、操作端末２０および認証装置２５である。訪問者ＩＤと当該訪問者の属性情報とを少なくとも記録しているＩＣカード等の認証媒体６５に対する読み込み動作を行うため、前記契約住宅における管理境界（例：玄関など）に設置されるのが認証装置２５である。よって、認証媒体６５の仕様や認証方式（指紋や虹彩等のバイオメトリクス認証含む）に応じたリーダ機能や、訪問者による訪問者ＩＤや暗号鍵の入力を受付ける液晶タッチパネル等の入出力インターフェイス、並びに契約住宅内の操作端末２０とのデータ通信機能を少なくとも備えている。無論、これに監視カメラやマイク、スピーカ、照明装置等が付帯するとより好適である。

【００１４】操作端末２０は、認証装置２５が読みとった、或いは入力を受け付けた、属性情報や訪問者ＩＤ、暗号鍵等を受け付けて、電子署名や適宜な暗号化を情報に施した上でインターネット等のネットワークを通じてＡＳＰサーバー１０に送信する。また、ＡＳＰサーバー

１０から、訪問者の認証結果や、異常発生の通知等を受信し、これに応じた、例えばセキュリティの解除／非解除動作や、警備実行機関への通報処理を実行する。上記操作端末２０または認証装置２５は、図２（ｂ）に示すように、例えばＸＭＬベースで記述されたアプリケーションプログラムでもって稼動するとする。このアプリケーションプログラムは、認証装置２５としてのカードリーダにおける認証媒体６５のアクセスや読取り動作をコントロールして、読取った情報を適宜加工しデータ通信に供する処理を行う他、契約住宅設置の各種センサー由来の検知データをＡＤ変換する処理や他種の警戒プログラムとの連携を図る処理を柔軟に実現する。

【００１５】警察機構や警備会社といった警備実行機関が備えるのが、警察端末４０、そして警備会社端末５０である。図２に示すように、例えば、前記管理会社とフランチャイズ契約を結んだローカル警備会社が備えるのが警備会社端末５０である。この警備会社端末５０はＡＳＰサーバー１０より担当エリア内の契約住宅の異常発生通知を受付け、他方この警備会社では実際にその契約住宅に警備員を急行させるなどの警備活動を行う。これにより、ＡＳＰサーバー１０を運営する管理会社が、地域ごとのローカル警備会社をフランチャイズ化することが可能となり、例えば全国的な広域セキュリティサービスをＡＳＰサービス化して低廉に運営することが可能となる。

【００１６】宅配等の契約住宅への訪問を伴う生業を営むのが前述の訪問会社である。この訪問会社が、備えるのが登録会社端末６０である。この端末６０では、自社の構成員を訪問者と定義してＩＤ登録して管理しており、例えばその訪問者ＩＤは、毎日更新されて不正使用の可能性低減が図られるとしてもよい。登録された訪問者が所持するのが、認証媒体６５である。ここには、所有者の訪問者ＩＤと、所属訪問会社名、所在地、連絡先、所属部署、担当管理者、社員ナンバー、生年月日などの属性情報とが登録デバイス６１により適宜更新・記録されている。形態としてはＩＣカード等のカード媒体が通常考えられるが、もちろんこれに限定されることはない。認証装置２５で対応可能な媒体であればいずれの媒体でも適用出来る。ここで登録された訪問者ＩＤや属性情報等は、ＡＳＰサーバー１０に送られて認証用情報データベース１１や認証局サーバー３０に登録される。

【００１７】なお、上記の各データベース１１、１２は、別々の記憶装置に設けられてネットワーク結合した各個独立のデータベースとして機能するものでもよいし、適宜組み合わせたり或いは１つの記憶装置に集約して設けてもよい。また　操作端末や認証装置、登録会社端末、警察端末、警備会社端末らは、一般のパーソナルコンピュータだけでなく、例えばネットワーク接続可能な携帯電話機、PDA、ゲーム機、ファックス機、デジタルＴＶなどネットワーク接続可能ないずれのコンピュータチップを備える機器でもよい。

【００１８】加えて、ＡＳＰサーバー１０と操作端末、認証局サーバー、登録会社端末、警察端末、警備会社端末らをつなぐネットワークに関して本実施形態では、インターネットとエクストラネットを用いたＷＡＮ（Wide Area Network）を想定するが、これに限らず、ＡＴＭ回線、パソコン通信回線、ＬＡＮ、無線ネットワークなど様々なネットワークを採用することも出来る。また、ＩＰＶＰＮなど仮想専用ネットワーク技術を用いれば、インターネットにおいても通信に関する高い機密性を効率よく実現できて好適である。

【００１９】図３は本実施形態におけるセキュリティ管理方法の実施手順を示す流れ図である。以下、本発明のセキュリティ管理方法の実際手順について説明する。契約住宅をある宅配業者（訪問会社）の配達員（訪問者）が訪れた場面を想定して説明を始める。この訪問者は、宅配業者から支給されている認証媒体（以下、ＩＣカード）６５を携行している。このＩＣカード６５に記録される訪問者ＩＤや属性情報、暗号鍵情報等は、当該ＩＣカード６５においては勿論、ＡＳＰサーバー１０の認証用情報データベース１１や認証局サーバー３０、警備会社端末５０、登録会社端末６０等において、図４に示すような手順で登録、変更ならびに削除が行われる。

【００２０】前記宅配業者に備わる登録会社端末６０で、配達員毎の属性情報が入力されると、その情報がＡＳＰサーバー１０に配達員毎に登録され、更にそれが認証局サーバー３０に転送されて登録される。認証局サーバー３０がこの配達員に関して電子証明書と暗号鍵（例：公開鍵ナンバー）を発行するなどして認証をしたならば、これを受けたＡＳＰサーバー１０は、この認証結果を記録して当該配達員の訪問者ＩＤを生成する。前記登録会社端末６０では、当該配達員に関する訪問者ＩＤと暗号鍵とをＡＳＰサーバー１０より受信し、前記登録デバイス６１を通じて当該配達員のＩＣカード６５にこれを書き込む。属性情報等の変更や削除、或いは配達員の登録自体を削除する場合にも、データ授受の流れは同様である。

【００２１】図５は本実施形態における有人アクセスプロセスの入室許可手順を示す説明図、図６は同入室不許可手順を示す説明図、図７は同緊急ケース手順を示す説明図、図８は同チェック手順を示す説明図、図９は有人アクセスの全プロセスを示す説明図、図１０は同無人アクセスの全プロセスを示す説明図である。以後、これらの図を参照しつつ説明を行うこととする。

【００２２】上記のようにして各種情報が登録されたＩＣカード６５は、前記配達員により、契約住宅の認証装置２５に挿入される。認証装置２５では、このＩＣカード６５をホールドすると共に読み込み動作を実施してＩＣカード６５に記憶されている属性情報を取得する。また、当該配達員による液晶タッチパネル等の入出力イン

ターフェイスにおけるキー入力等を受け付けて訪問者ＩＤや暗号鍵情報を取得する。但しこの時点では、この訪問者ＩＤや暗号鍵が真正のもの否かは不明である。

【００２３】認証装置２５が上記のように取得した属性情報等は、例えば操作端末２０を介してＡＳＰサーバー１０に送信される。この時、属性情報に対して前記暗号鍵でもって電子署名を付し、暗号化した上でネットワーク上にデータ送信するとすれば好適である。ＡＳＰサーバー１０ではこれを受信し、受け付けた訪問者ＩＤと署名付き属性情報、暗号鍵を認証用情報データベース１１に記録する（ｓ３０１）。そして、記録した暗号鍵と署名付き属性情報とを認証局サーバー３０に送信してその認証結果を入手することで該当訪問者の正当性を認証する。或いは、訪問者あるいはＩＣカード６５各個に対応付けて訪問者ＩＤを記録した前記認証用情報データベース１１における認証を実行して配達員の正当性を認証する（ｓ３０３）。操作端末２０から受信した属性情報が署名付きでないとすれば、暗号鍵でもって電子署名を施し、また暗号化処理を図っておく（ｓ３０２）。

【００２４】なお、前記の暗号鍵は、ＡＳＰサーバー１０が、配達員（登録者）に所定間隔で更新・発行するスレーブキーであるとし、このスレーブキーに関する認証装置２５における訪問者の入力を受付けて（ｓ３０１’）一次認証を行う（ｓ３０２’）としてもよい。この場合、このスレーブキーに対応する配達員（登録者）に対して認証局サーバー３０から発行されたマスターキーを認証用情報データベース１１から抽出する（ｓ３０３’）。そしてこのマスターキーで属性情報に署名を付して認証局サーバー３０に送信し、その認証結果を取得する二次認証を実行することが必要となる。これにより、前記宅配業者を辞めてしまった元配達員がその後に不正にＩＣカード６５を利用するなどの状況が生じても、例えばスレーブキーが日々更新されているとすれば、契約住宅等への不正侵入を阻止出来るのである。一方で、例えば宅配業者毎に所定数のマスターキーを予め配布しておいて、このマスターキーに紐付けるスレーブキーのみをＡＳＰサーバー１０等で自在に変更するとすれば、認証局サーバー３０に対し配達員の増減に伴ってその訪問者ＩＤの発行や属性情報の登録手続を一々行う手間を省略することにもつながる。

【００２５】認証結果が正常であれば、その認証結果を該当契約住宅の操作端末２０に送信する（ｓ３０５）。契約住宅内においてこれを認識した例えば主婦は、この配達員が前記管理会社が認めた宅配業者の真正なる配達員であることを確認し、例えばその宅配物を受け取るべく、玄関ロックとそのセキュリティを一時解除する動作（例：解除キーを操作端末２０に入力する）を行う。ＡＳＰサーバー１０は、管理境界内（つまり玄関より内側）への配達員の受け入れを可としたこの事象に応じて、操作端末２０で行われたセキュリティの解除動作情報を当該操作端末２０から受信して動作記録データベース１２に記録する（ｓ３０６）。

【００２６】或いは、この契約住宅が無人である場合、ＡＳＰサーバー１０が前記認証結果を契約住宅の家人が所持する携帯端末２７に送信し、そのセキュリティ管理解除動作を受付ける一方で、それに応じて当該契約住宅のセキュリティ解除動作を行うとしてもよい。また、家人の判断を待たずに、予め定められた解除条件に合致すればＡＳＰサーバー１０がセキュリティ解除指令を操作端末２０に発するとしてもよい（このような配達員の契約住宅内への入室が許可される場合の手順は図５に示している）。

【００２７】他方、認証結果が不良で、真正な配達員であると認証出来なかったった場合、受け付けた訪問者ＩＤ又は暗号鍵が、緊急コードであるか判定する（ｓ３０４’）。この緊急コードは、例えば真正な配達員が、配達途中に何者かに脅迫されて契約住宅への訪問を強要されている場合などに、この真正な配達員が認証装置２５で入力する緊急用のナンバーである。ここで緊急コードであると判断されたならば、この配達員は非登録の配達員（非登録訪問者）であると判断され、なにがしかの緊急事態が生じていることが容易に推定される。この非登録訪問者による訪問事象は、少なくともＡＳＰサーバー１０において記録され（ｓ３０５’）、その旨が該当契約住宅における操作端末２０に通知される（ｓ３０６’）。そして、認証装置２５に「しばらくお待ち下さい」といった待機文を表示すべくＡＳＰサーバー１０は指令を発して警備員の配備時間を稼ぎつつ、即座に警備実行機関への通報等を行う（ｓ３１１）。勿論、この場合、セキュリティは非解除のままとなって、その旨が動作記録データベース１２に記録される（このような配達員の契約住宅内への入室が不許可である場合、および緊急ケースについての手順は図６および７に示している）。

【００２８】一方、契約住宅内に配達員が受け入れられた時点、つまりＡＳＰサーバー１０がセキュリティ解除情報を動作記録データベース１２に記録した時点から、管理境界内における該当配達員の滞在時間が開始したと認識される。ＡＳＰサーバー１０は、当該契約住宅におけるこの滞在に関して、滞在時間を測定するタイマー設定を行い時間測定をスタートさせる（ｓ３０７）。

【００２９】この配達員の滞在時間が予め定めた閾値を越えた場合（ｓ３０８）は、例えば通常の配達業務にかかるであろう時間を大幅に越えて何らかの問題行動が起きている惧れもあるとして、その閾値超過発生事象を該当操作端末２０または認証装置２５に通知する（ｓ３０９）。この通知に対して、操作端末２０または認証装置２５からの応答情報が何ら無かった場合、或いは問題発生を示唆する応答情報を受信したＡＳＰサーバー１０は、管理境界内での某かの異常発生が有ると判断し（ｓ

３１０）、契約住宅に設置された所定の警備装置（監視カメラや警告通知スピーカなど）に適宜な警備動作を行うべく警備指令を通知する。或いは、警察端末４０や担当エリアに存在するローカル警備会社の警備会社端末５０に、警備員出動依頼など対処依頼通知を行う（ｓ３１１）。

【００３０】操作端末２０等からの応答情報を検証した結果、或いは前記の警備実行機関の警備活動の結果、特に契約住宅に問題は発生しておらず、例えば単に荷下ろし作業に手間取っているだけといった状況が判断できたとすれば、この契約住宅における配達員の今回の滞在に対し設定されていたタイマーを延長する等のセキュリティリセット処理を行う（ｓ３１３）（このような滞在時間のチェックプロセスについては図８に示している）。

【００３１】当該契約住宅における真正な配達員の作業が完了すれば、玄関から退出する時が到来する。この時、ＡＳＰサーバー１０は、この契約住宅にいる家人が操作端末２０に行う操作もしくは配達員自身が認証装置２５に行う操作を、この配達員の退出事象として前記操作端末２０または認証装置２５から受信する。そしてこれを動作記録データベース１２に記録すると共に（ｓ３１４）、この配達員のＩＣカード６５に対するホールド解除指令を操作端末２０または認証装置２５に送信し（ｓ３１５）、処理は終了する。

【００３２】本発明に係る実施の形態としては、前記目的を達成すべく、次の通りとしてもよい。前記セキュリティ管理方法において、前記ＩＤ等受付手順で、訪問者個々に割り当てられた暗号鍵と当該訪問者の属性情報とを記録している認証媒体に対する、前記認証装置による読み込み動作によって得られた属性情報と、当該訪問者による認証装置における入力を受け付けて得た暗号鍵と、この暗号鍵で電子署名を施した署名付き属性情報とを、この認証装置から受付け、前記認証手順において、前記暗号鍵および署名付き属性情報をデータベースに記録すると共に、当該暗号鍵と署名付き属性情報とを認証局に送信してその認証結果を入手することで該当訪問者の正当性を認証することとする。

【００３３】また、前記セキュリティ管理方法において、サーバーが訪問者になるであろう登録者に所定間隔でスレーブキーを更新発行し、このスレーブキーに関する認証装置における訪問者の入力を受付けて一次認証を行うと共に、このスレーブキーに対応する登録者に対して認証局から発行されたマスターキーをデータベースから抽出して認証局に送信し、その認証結果を取得する二次認証を実行することとする。

【００３４】更に、前記セキュリティ管理方法において、セキュリティ解除情報を記録した時点から、管理境界内における該当訪問者の滞在時間が開始したと認識し、この滞在時間が予め定めた閾値を越えた場合、その閾値超過発生事象を、該当する操作端末または認証装置に通知する超過発生事象通知手順と、通知した超過発生事象に対する、操作端末または認証装置からの応答情報を受信して或いは応答情報の有無でもって、管理境界内での異常発生の有無を判断する異常発生判断手順と、異常が発生していると判断したならば、管理境界に設置された所定の警備装置に適宜な警備動作を行うべく警備指令を通知するか、或いは、警察や予め契約してある警備会社等の警備実行機関に対処依頼通知を行う対応通知手順とを含むこととする。

【００３５】また、前記セキュリティ管理方法において、前記ＩＤ等受付手順において受け付けた、訪問者ＩＤ、暗号鍵、またはスレーブキーのいずれかが、登録済みの正当な訪問者が緊急時に入力すべき緊急コードである場合、これを認証装置または操作端末から受け付けたサーバーは、非登録の訪問者である旨を前記操作端末に通知すると共に、前記対応通知手順を実行することとする。

【００３６】更に、前記セキュリティ管理方法において、建造物或いは建造物内外の特定エリアといったセキュリティ管理の対象が存在するエリア毎に担当警備会社や警察等の警備実行機関を関連づけするとし、当該警備実行機関の備える警備機関端末に対し、担当エリアに存在する操作端末または認証装置に対しなされる各種情報や指令の通知や記録手順を同様に実行することとする。

【００３７】また、前記セキュリティ管理方法を実現するシステムであって、訪問者個々に割り当てられたＩＤと当該訪問者の属性情報とを少なくとも記録している認証媒体に対する、前記管理境界に設置された認証装置による読み込み動作によって得られた属性情報と、当該訪問者による認証装置における入力を受け付けて得た訪問者ＩＤとを、この認証装置から受付けるＩＤ等受付装置と、前記認証装置から受け付けた訪問者ＩＤと属性情報とをデータベースに記録するとともに、訪問者あるいは認証媒体各個に対応付けて訪問者ＩＤを記録したデータベースにおける認証、または前記訪問者ＩＤの起源となっている認証局への認証依頼とその結果の取得を実行することで該当訪問者の正当性を認証する認証装置と、前記認証処理の結果を、該当管理境界内に設置されている操作端末に送信すると共に、管理境界内への訪問者の受け入れ可否に応じて当該操作端末で行われたセキュリティの解除／非解除動作情報を操作端末から受信してデータベースに記録するセキュリティ解除等記録装置と、受け入れられた訪問者が管理境界から退出する旨の事象を前記操作端末または認証装置から受信してこれをデータベースに記録すると共に、この訪問者の認証媒体に対するホールド解除指令を操作端末または認証装置に送信する退出記録装置とを備えることを特徴とするセキュリティ管理システムをなすこととする。

【００３８】更に、建造物或いは建造物内外の特定エリアの管理境界における訪問者の出入管理を、ネットワー

13

クを介したサーバー上で実現するプログラムであって、訪問者個々に割り当てられたＩＤと当該訪問者の属性情報とを少なくとも記録している認証媒体に対する、前記管理境界に設置された認証装置による読み込み動作によって得られた属性情報と、当該訪問者による認証装置における入力を受け付けて得た訪問者ＩＤとを、この認証装置から受付けるＩＤ等受付手順と、前記認証装置から受け付けた訪問者ＩＤと属性情報とをデータベースに記録するとともに、訪問者あるいは認証媒体各個に対応付けて訪問者ＩＤを記録したデータベースにおける認証、または前記訪問者ＩＤの起源となっている認証局への認証依頼とその結果の取得を実行することで該当訪問者の正当性を認証する認証手順と、前記認証処理の結果を、該当管理境界内に設置されている操作端末に送信すると共に、管理境界内への訪問者の受け入れ可否に応じて当該操作端末で行われたセキュリティの解除／非解除動作情報を操作端末から受信してデータベースに記録するセキュリティ解除等記録手順と、受け入れられた訪問者が管理境界から退出する旨の事象を前記操作端末または認証装置から受信してこれをデータベースに記録すると共に、この訪問者の認証媒体に対するホールド解除指令を操作端末または認証装置に送信する退出記録手順とを備えることを特徴とするセキュリティ管理プログラムをなすこととする。

【００３９】また、前記セキュリティ管理プログラムを記録したコンピュータ読み取り可能な記録媒体をなすこととする。

【００４０】

【発明の効果】本発明によれば、侵入事件等の発生を簡便確実かつ低コストのもとで抑制し、機能拡張等の柔軟＊

14

＊性に富んだセキュリティ管理方法およびシステムを提供可能となる。

【図面の簡単な説明】

【図１】本実施形態におけるセキュリティ管理システムとしてのＡＳＰサーバーを含むネットワーク概要図である。

【図２】本実施形態におけるセキュリティ管理方法を適用したビジネスモデルを示す説明図である。

【図３】本実施形態におけるセキュリティ管理方法の実施手順を示す流れ図である。

【図４】本実施形態における出入室者の登録、変更および削除手順を示す説明図である。

【図５】本実施形態における有人アクセスプロセスの入室許可手順を示す説明図である。

【図６】本実施形態における有人アクセスプロセスの入室不許可手順を示す説明図である。

【図７】本実施形態における有人アクセスプロセスの緊急ケース手順を示す説明図である。

【図８】本実施形態における有人アクセスプロセスのチェック手順を示す説明図である。

【図９】本実施形態における有人アクセスの全プロセスを示す説明図である。

【図１０】本実施形態における無人アクセスの全プロセスを示す説明図である。

【符号の説明】

ｓ３０１　ＩＤ等受付手順

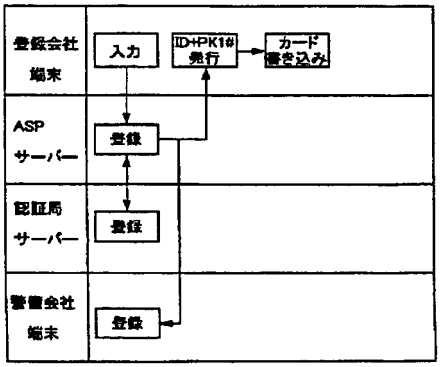
ｓ３０３　認証手順

ｓ３０６　セキュリティ解除等記録手順

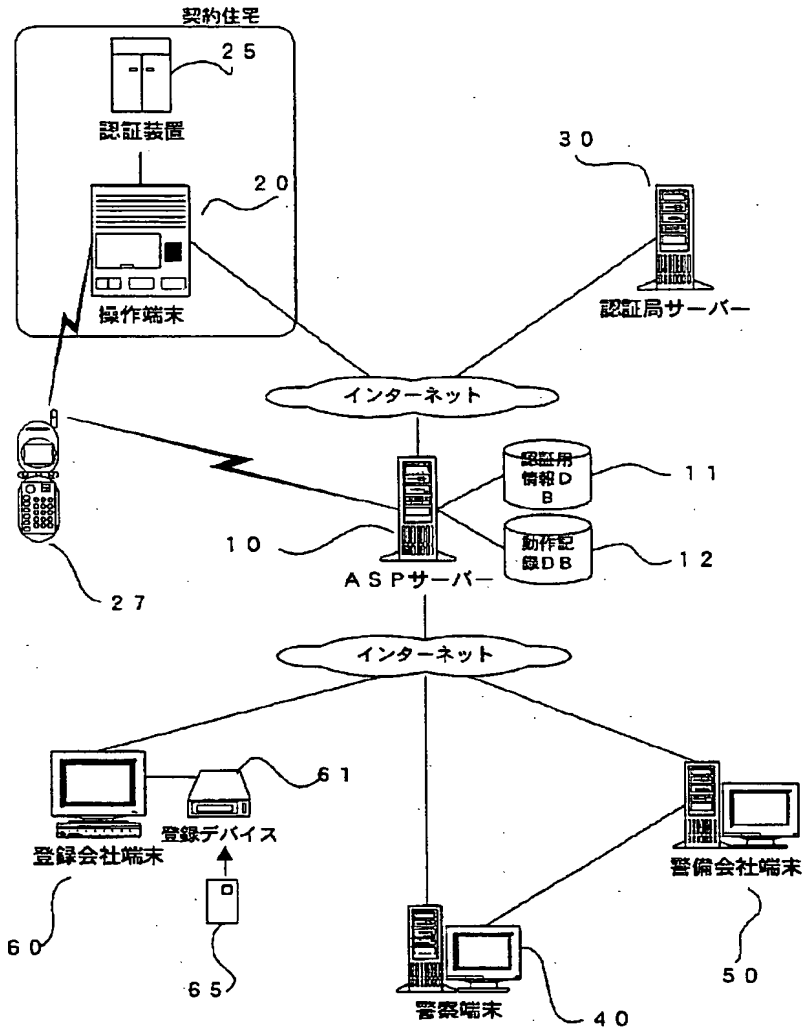
ｓ３１５　退出記録手順

【図４】

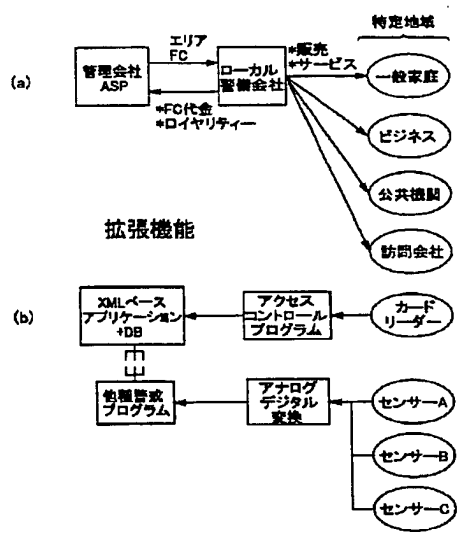
出入室者登録、変更、削除



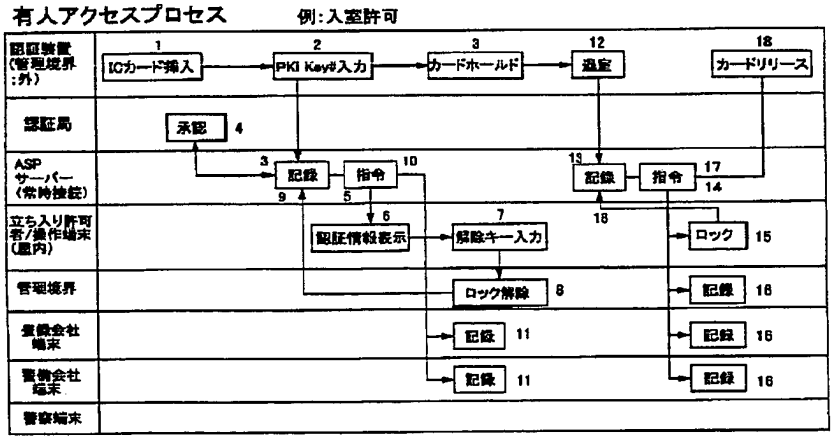
【図１】


契約住宅
２５
認証装置
２０
操作端末
３０
認証局サーバー
インターネット
認証用情報ＤＢ
１１
１０
ＡＳＰサーバー
動作記録ＤＢ
１２
２７
インターネット
６１
登録デバイス
登録会社端末
６０
６５
警備会社端末
５０
警察端末
４０

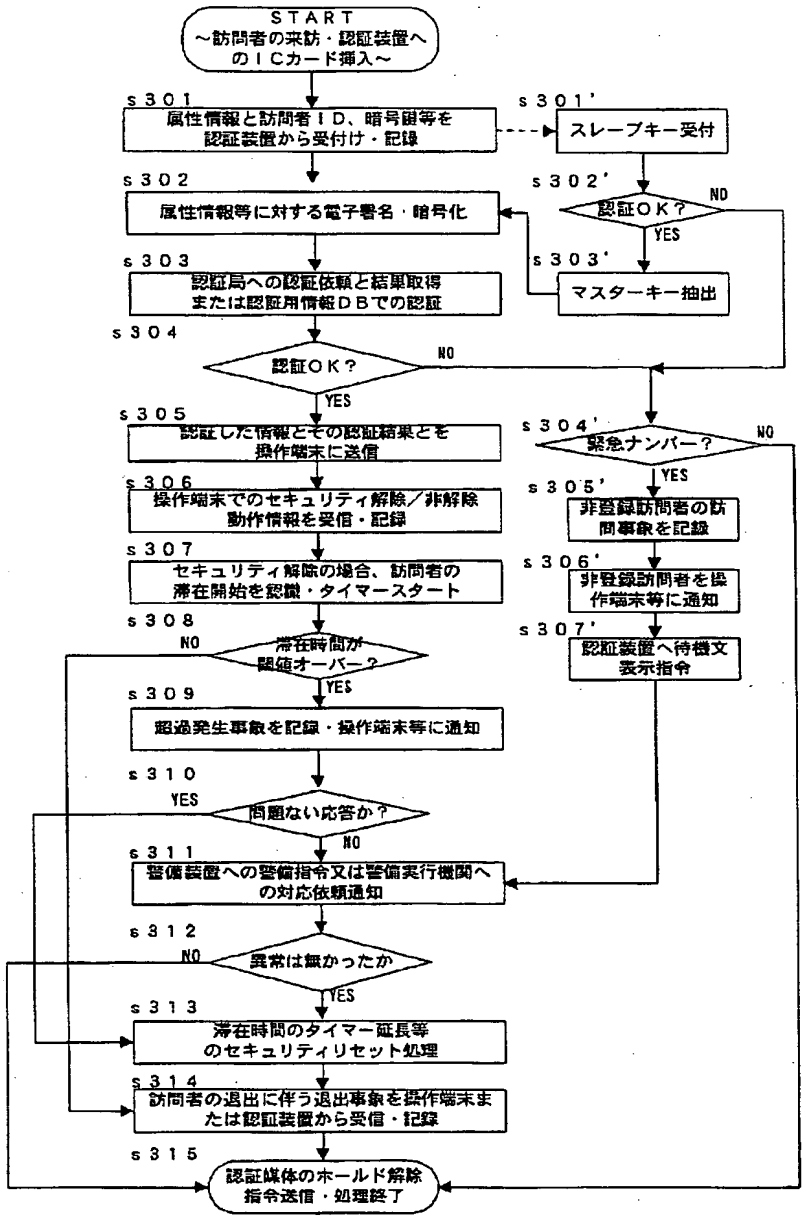
【図２】


フランチャイズ制
特定地域
(a)
管理会社
ASP
エリア
FC
ローカル
営業会社
*販売
*サービス
一般家庭
ビジネス
公共機関
訪問会社
*FC代金
*ロイヤリティー
拡張機能
(b)
XMLベース
アプリケーション
+DB
アクセス
コントロール
プログラム
カード
リーダー
他種言或
プログラム
アナログ
デジタル
変換
センサーA
センサーB
センサーC

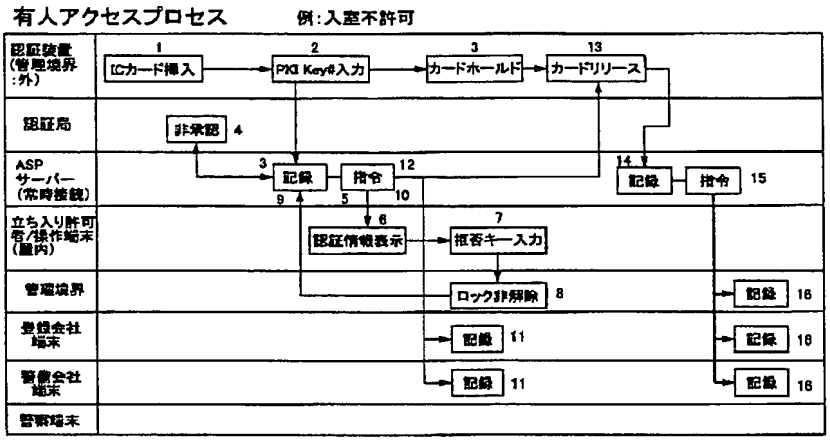
【図５】


有人アクセスプロセス
例:入室許可
認証装置
(管理境界
:外)
1
ICカード挿入
2
PKI Key#入力
3
カードホールド
12
退室
18
カードリリース
認証局
承認
4
ASP
サーバー
(常時接続)
3
記録
指令
10
13
記録
指令
17
14
9
4
5
6
18
立ち入り許可
者/操作端末
(屋内)
認証情報表示
7
解除キー入力
ロック
15
管理境界
ロック解除
8
記録
16
警備会社
端末
記録
11
記録
16
警備会社
端末
記録
11
記録
16
警察端末

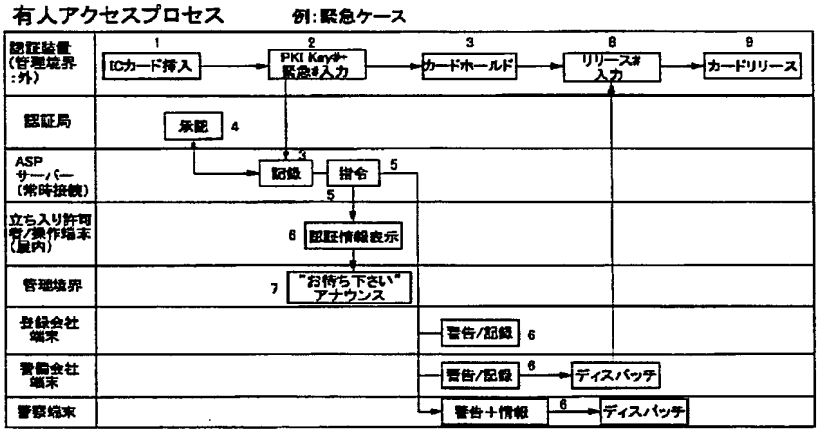
【図３】


ＳＴＡＲＴ
～訪問者の来訪・認証装置へのＩＣカード挿入～
ｓ３０１
属性情報と訪問者ＩＤ、暗号鍵等を認証装置から受付け・記録
ｓ３０１'
スレーブキー受付
ｓ３０２
属性情報等に対する電子署名・暗号化
ｓ３０２'
認証ＯＫ？
NO
YES
ｓ３０３
認証局への認証依頼と結果取得または認証用情報ＤＢでの認証
ｓ３０３'
マスターキー抽出
ｓ３０４
認証ＯＫ？
NO
YES
ｓ３０５
認証した情報とその認証結果とを操作端末に送信
ｓ３０４'
緊急ナンバー？
NO
YES
ｓ３０６
操作端末でのセキュリティ解除／非解除動作情報を受信・記録
ｓ３０５'
非登録訪問者の訪問事象を記録
ｓ３０７
セキュリティ解除の場合、訪問者の滞在開始を認識・タイマースタート
ｓ３０６'
非登録訪問者を操作端末等に通知
ｓ３０８
滞在時間が閾値オーバー？
NO
YES
ｓ３０７'
認証装置へ待機文表示指令
ｓ３０９
超過発生事象を記録・操作端末等に通知
ｓ３１０
問題ない応答か？
YES
NO
ｓ３１１
警備装置への警備指令又は警備実行機関への対応依頼通知
ｓ３１２
異常は無かったか
NO
YES
ｓ３１３
滞在時間のタイマー延長等のセキュリティリセット処理
ｓ３１４
訪問者の退出に伴う退出事象を操作端末または認証装置から受信・記録
ｓ３１５
認証媒体のホールド解除指令送信・処理終了

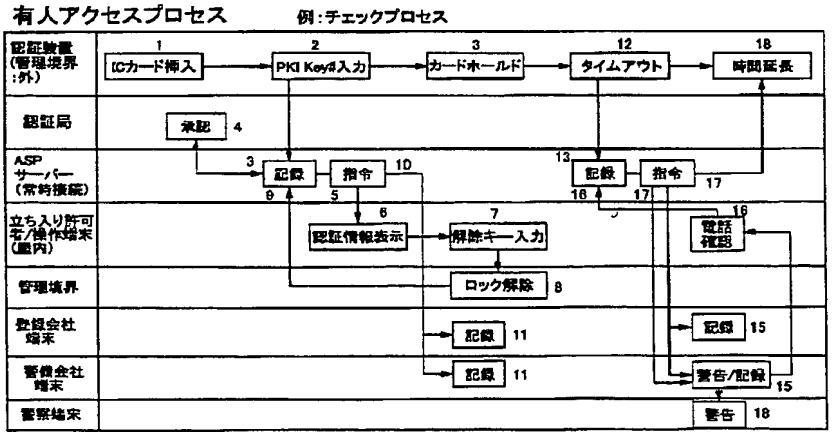
【図６】


有人アクセスプロセス
例：入室不許可
認証装置（管理境界：外）
認証局
ASPサーバー（常時接続）
立ち入り許可者/操作端末（屋内）
管理境界
登録会社端末
警備会社端末
警察端末
ICカード挿入
PKI Key#入力
カードホールド
カードリリース
非承認
記録
指令
認証情報表示
拒否キー入力
ロック非解除

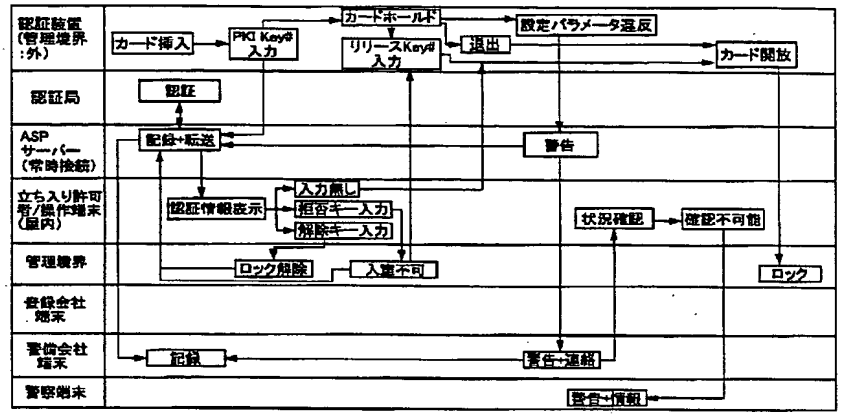
【図７】


有人アクセスプロセス
例：緊急ケース
認証装置（管理境界：外）
認証局
ASPサーバー（常時接続）
立ち入り許可者/操作端末（屋内）
管理境界
登録会社端末
警備会社端末
警察端末
ICカード挿入
PKI Key#緊急#入力
カードホールド
リリース#入力
カードリリース
承認
記録
指令
認証情報表示
"お待ち下さい"アナウンス
警告/記録
ディスパッチ
警告＋情報

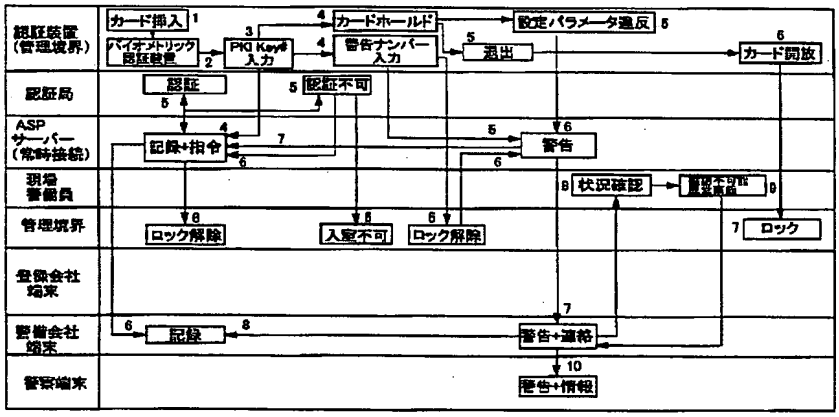
【図８】


有人アクセスプロセス
例：チェックプロセス
認証装置（管理境界：外）
認証局
ASPサーバー（常時接続）
立ち入り許可者/操作端末（屋内）
管理境界
登録会社端末
警備会社端末
警察端末
ICカード挿入
PKI Key#入力
カードホールド
タイムアウト
時間延長
承認
記録
指令
認証情報表示
解除キー入力
電話確認
ロック解除
警告/記録
警告

【図９】



【図１０】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
		H04L 9/00	673E 675A

(72)発明者　高橋　直紀
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション事業部内

Fターム(参考)　5B085 AA08 AE02 AE06 AE12 AE23 BG03 BG07
5C087 AA44 BB03 BB12 BB18 CC52 DD05 DD06 DD24 EE07 FF01 FF04 FF19 FF20 GG03 GG08 GG10 GG18 GG20 GG21 GG23 GG30 GG36 GG51 GG57
5J104 AA07 AA09 KA01 MA01 PA15